17 April 2003

Standard Operating Procedures
For Scanning NPS Information Systems

Purpose:

This document provides the procedures for scanning and monitoring unclassified NPS Information Systems. NPS Information Systems include the networks, all computer systems or applications on the network or stand-alone system.

Responsibilities:

The NSG is the group responsible for running intrusion detection tools against the NPS information systems. There are several reasons for conducting scans on NPS information systems.

1. As a preventative measure to ensure our systems are configured in accordance with the Department of Navy standards as well as industry standards. The NSG will conduct scheduled scans of the networks and production systems on a routine basis to confirm that the patches and configurations are still valid.

2. As a tool to confirm that a system is configured correctly. Any system administrator can request a scan be conducted against their system. The resulting report can be used by the system administrator to either fix any problems or document the configuration of the system.

3. To monitor the networks. The tools and the placement of NSG intrusion detection servers will give the ITACS a method for monitoring the network. Monitoring is a valuable tool to detect problems as well as to collect performance data.

The ITACS organization is responsible for the operation of the network and the information systems that are either stand-alone or connected to the network. ITACS designs the system, implements and maintains the NPS information security policies. ITACS is responsible for adhering to the information security policies. The ITACS staff uses system logs as well as various network monitoring tools to monitor the system performance.

The Information System Security Manager is responsible for the information system security at NPS. Information systems include the networks, computer systems (either stand-alone or connected to the network) and applications. Routine scanning of information systems will ensure that NPS is compliant with security policies and best practices.

Operating Procedures:

There are several scenarios under which NPS systems will be scanned:

1. **Routine periodic scanning**. All routine scanning (to include the NSG published audit schedule) of NPS information systems will be coordinated, prior to the scan, with the ISSM, the ITACS manager and the system administrator responsible for the system. The scan results will be provided to the same list of personnel.

2. **Scan on request**. These types of scans will be requested by a system administrator to validate the system configuration and identify vulnerabilities. The time of the scan will be coordinated between the NSG and the system administrator. The scan results will be provided to the system administrator.

3. **Red Cell scanning**. Red cell scanning will be conducted by the NSG annually or at the request of leadership. The Superintendent and Command Information Officer/DAA will have final approval on any and all red cell activity conducted by the NSG. The Superintendent, the Chief Security Officer and the Command Information Officer will be informed of the time frame of the test. The Chief Security Officer will act as the coordinator. Appendix A will be completed prior to any red cell activity. With the exception of the personnel noted above no one will be informed. There are two purposes for the red cell evaluation:

   a. Technical evaluation. This type of evaluation checks the configuration of the systems, to ensure all patches have been applied and security configurations have been completed.

   b. Administrative evaluation. This type of test would test the processes that are in place to ensure that security policies are being practiced. This evaluation checks the awareness of technicians and the reporting procedures.

Notification:

The NSG will provide the results of any scans to the system administrator, the ITACS manager and the ISSM. In the case where the scan identifies a problem, ITACS, the NSG and the ISSM will meet to determine the impact and the required action. Depending on the problem or vulnerability identified, ITACS will inform the user base regarding the impact on services. Refer to the **Standard Operating Procedure for Responding to an Information System Security Incident** for the reporting procedures.

In the case of the red cell evaluation, the detailed results will be provided to the system administrator, the ITACS Manager and the ISSM, so any corrective action can be taken. The NSG will prepare an executive summary of the results for leadership.

Note: The results of a scan that identifies vulnerabilities should be handled as FOUO and should be evaluated to determine if a higher classification is necessary. Processing the results on an unclassified system should be considered prior to typing the results.

TERRI BRUTZMAN
Information Systems Security Manger

CHRISTINE M. CERMAK
Designated Approving Authority

Appendix A

Date

SUBJECT: Naval Postgraduate School Local Area Network Security Audit

Attachment: Naval Postgraduate School Local Area Network Security Audit Waiver

By request of the Superintendent, Naval Postgraduate School (NPS), the NPS Network Security Group will conduct a security audit of the NPS unclassified Local Area Network (LAN). The purpose of the audit will be to examine and/or analyze (the technical security safeguards of the Automated Information System (AIS) or both the technical and administrative safeguards and practices of the Automated Information Systems (AIS)).

(The following paragraph will describe what type of scanning will be accomplished. The following is an example.)
In order to audit the AIS, several types of scanning will be required. The scanning will be in the form of IP packets passing between the NSG lab auditing station and the NPS LAN. A significant amount of TCP and UDP traffic could be generated in the process. Specifically, all ports with UDP, SYN half-open, and full-connect scans will be targeted.

The assessment team will remain on-site while the scan is active, and can be reached in one of the following ways:

(NSG Team members to be noted here.)
NSG
Phone number
e-mail address

The above members of the assessment team will be happy to respond to any concerns or questions, or provide more detail of the scanning if required.

ATTACHMENT 1: Naval Postgraduate School LAN Security Audit Waiver

Company Name: **Naval Postgraduate School**

Contact Name: **Admiral Ellison**
Captain Robert Simeral
Dr. Christine Cermak

IP Addresses to be audited: **TBD**

Please sign and date below acknowledging your acceptance to the following statements:

(1) I am the authorized administrator of the hardware to be audited.